**Positionspapier der SPD-Bundestagsfraktion**

# Stärkung des digitalen Immunsystems

Immer mehr Lebensbereiche sind von Vernetzung und digitalen Technologien erfasst. Insbesondere durch die zunehmende Digitalisierung der Wirtschaft entstehen immer größere Datenmengen („Big Data“). Diese Entwicklung eröffnet Möglichkeiten für neue Geschäftsmodelle und birgt Optimierungspotential für Produktionsprozesse.

Damit einhergehen auch Fragen der Sicherheit der Informationstechnologie und der IT-Infrastrukturen, der Sicherheit und Funktionsfähigkeit der Steuerungen und Dienstleistungen sowie des Schutzes vor kriminellem Missbrauch und Angriffen.

Laut aktuellem Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für 2015 ist die Gefährdungslage der IT-Sicherheit in vielen Bereichen als hoch zu bewerten. Cyberkriminalität, Industriespionage und -sabotage sind zu einem weiter wachsenden Problem geworden. Nach Angaben des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) sind gut die Hälfte (51 Prozent) aller Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von Cyberkriminalität geworden. Mittelständische Unternehmen sind mit 61 Prozent besonders stark von Spionage- oder Sabotageakten betroffen. Der jährliche Schaden für die deutsche Wirtschaft wird auf rund 51 Milliarden Euro geschätzt.

Ohne Datensicherheit können wir aber insbesondere unsere kleinen und mittelständischen Unternehmen nur schwer davon überzeugen, dass die Digitalisierung ihrer Geschäfte erforderlich ist, um wettbewerbsfähig zu bleiben. IT-Sicherheit wird daher zu einer wesentlichen Voraussetzung für Innovationen und Wachstum.

Auch in Unternehmen muss der Gedanke wachsen, dass das Vertrauen der Kunden in einen sicheren Umgang mit Daten und die Achtung der Privatsphäre ein entscheidender Wettbewerbsvorteil sein kann. Staat und Wirtschaft müssen gemeinsam dafür sorgen, dass die immer komplexeren Systeme vor Missbrauch und unbefugtem Zugriff, vor Manipulation und vor Ausspähung geschützt werden. Nur wenn es gelingt, diesen Herausforderungen zu begegnen, wird die Digitalisierung gesellschaftlich akzeptiert und wirtschaftlich erfolgreich.

Die erfolgreiche Digitalisierung der Wirtschaft ist entscheidend für die weitere wirtschaftliche Entwicklung Deutschlands. Eine sichere digitale Infrastruktur und der Schutz vor Cyberkriminalität sind existentiell für unseren leistungsstarken Mittelstand und unsere moderne Industrie. Die Frage nach der Sicherheit im digitalen Raum wird in den kommenden Jahren noch weiter an Bedeutung gewinnen und sich zu einem wichtigen Wettbewerbs- und Standortfaktor entwickeln. Deutschland muss zu einem sicheren digitalen Hafen für Unternehmen werden und „Cybersicherheit Made in Germany“ zum Exportschlager und Standortvorteil weiterentwickelt werden. Deutschland zum Leitmarkt und zum Leitanbieter für IT-Sicherheit zu machen, ist unser Ziel. Cyberangriffe durch organisierte Kriminalität oder Industriespionage durch Konkurrenzunternehmen oder andere Staaten dürfen nicht zur Belastung für deutsche Unternehmen werden.

Insbesondere im Bereich der Industrie 4.0 befindet sich Deutschland an einem Scheideweg: Nutzen KMU die Vorteile einer vernetzten Produktion oder Schrecken sie vor den Investitionen und den potentiellen Gefahren digitaler Technologien zurück. Die Modernisierung unserer Wirtschaft darf nicht aus Angst vor Angriffen auf potentiell angreifbare und gefährdete Systeme ge-

hemmt werden. Datensicherheit und -schutz in Deutschland müssen weiter nachhaltig und effektiv gestärkt werden. Gerade mittelständische Unternehmen müssen in die Lage versetzt werden, Gefahren zu erkennen und sich davor zu schützen, um die mit der Digitalisierung verbundenen Chancen im vollen Umfang nutzen zu können.

Der Staat und die Unternehmen müssen gemeinsam für ein starkes digitales Immunsystem eintreten. Der Staat muss den rechtlichen Rahmen zu Verhinderung und Verfolgung von Cyberkriminalität setzen. Darüber hinaus muss er die Behörden und Institutionen adäquat ausstatten, um eine Strafverfolgung sowie die Beratung zur Kriminalitätsprävention zu ermöglichen. Staat und Unternehmen müssen der Cyberkriminalität gemeinsam den Kampf ansagen.

Die Unternehmen müssen Angebote in Form von „Hilfe zu Selbsthilfe und zum Selbstschutz“ durch den Staat erhalten. Konkrete, kompetente Ansprechpartner, die bei Sicherheitsfragen beraten und informieren, sind von großer Bedeutung. Sie müssen Unternehmen dabei unterstützen, entsprechende Schutzmaßnahmen zu ergreifen, die das Datensicherheitsniveau signifikant erhöhen. Sicherheit und Datenschutz sind möglichst von Beginn der Produktentwicklung und der Konzeption von Prozessen an mitzudenken.

Einen wichtigen Schritt, um diesen Herausforderungen zu begegnen und dem Ziel, mehr Sicherheit im digitalen Raum zu schaffen, gerecht zu werden, sind wir in mit der Verabschiedung des IT-Sicherheitsgesetzes gegangen. Weitere Schritte müssen, im Rahmen der zur Verfügung stehenden Haushaltsmittel, folgen:

*Wir brauchen wie in der bisherigen Produktwelt auch für digitale Produkte und Dienstleistungen eine eindeutige Haftungskette.*

- Durch eine entsprechende Regelungen im ProdHaftG und ProdSG ist klarzustellen, dass auch Software und Softwaredienste bzw. Dienstleistungen im Hinblick auf die Speicherung, Nutzung und Verarbeitung von Daten, Produkte i. S. d. Gesetze sind, um so auch Software zum Download sowie Cloud-Dienste mit aufzunehmen.
- Das ProdSG muss dahingehend geändert werden, dass auch das Eigentum geschützt ist. Gleichzeitig wollen wir in diesem Zusammenhang prüfen, ob im Schadensfall auch für Vermögensschäden Schadensersatz zu leisten ist.

*Die Informations- und Meldepflichten der Hersteller über Sicherheitsmängel müssen ausgebaut und das BSI in seiner Dienstleistungsfunktion gestärkt werden. Darum wollen wir:*

- Über die Pflichten des BDSG hinaus die Anbieter von Cloud-Diensten dazu verpflichten, ihre Kunden über erkannte besonders schwere Angriffe zu informieren, damit diese ihren Schutz und ihre Selbstschutzinstrumente entsprechend anpassen können.
- Im IT-Sicherheitsgesetz sind in einem weiteren Schritt die Soft- und Hardwarehersteller in die Meldepflicht gegenüber dem BSI aufzunehmen, wenn Mängel oder Sicherheitslücken beim Anwender zu Schäden an Leib, Leben, Gesundheit und Eigentum führen können.
- Das BSI soll die Verpflichtung erhalten, öffentliche Warnungen unter Nennung des Produktes und Herstellers sowie gegebenenfalls der Sicherheitslücke auszusprechen, wenn

nach Information an den Hersteller der Software und nach einem angemessenen Zeitablauf die Sicherheitslücke nicht geschlossen wurde.

- Das BSI soll in seiner neutralen Rolle und Beratungsfunktion gestärkt werden. Seine weisungsabhängige Eingliederung in den Geschäftsbereich und die Dienstaufsicht des BMI erschwert seine neutrale Aufgabenwahrnehmung gegenüber anderen Behörden des Bundes und als Ansprechpartner und Berater für Bürgerinnen und Bürger sowie Unternehmen.

*Wir wollen die "Selbstimmunisierungsfähigkeit" der "digitalen Welt" stärken:*

- Durch Schaffung einer beim BSI angegliederten Meldestelle, bei der jeder entsprechende Lücken – auch anonym oder pseudonym – melden kann.
- Durch Stärkung der IT-Sicherheitsforschung im Bereich der digitalen Infrastrukturen und Sicherstellung der digitalen Souveränität beim Infrastrukturausbau.
- Indem auch jene Unternehmen, die nicht als kritische Infrastrukturbetreiber gesetzlichen Verpflichtungen unterliegen, ihr Datensicherheitsniveau verbessern. Dafür müssen wir u. a. die Angebote der Initiative „IT-Sicherheit in der Wirtschaft“ gemeinsam mit Partnern aus Wirtschaft und Wissenschaft weiter ausbauen.
- Indem die für Cloud-Angebote erarbeitete Datenschutzzertifizierung im Rahmen des Technologieprogramms „Trusted Cloud“ die Grundlage für ein europäisches Label bilden wird.
- Durch die Entwicklung einer Landkarte der digitalen (Sicherheits-)Kompetenzen. So sollen sich Unternehmen einen schnellen Überblick verschaffen können, auf welche digitalen Fähigkeiten und Schlüsselkompetenzen sie zurückgreifen können. Darauf aufbauend, muss eine Identifikation und Analyse über Kompetenzlücken stattfinden, die ermöglicht, Schlüsseltechnologien und -kompetenzen, die zum Erhalt und Aufbau digitaler Souveränität und Sicherheit benötigt werden, gezielt zu fördern und die vorhandenen Kompetenzlücken zu schließen.
- Durch eine gesetzliche Regelung, die das verantwortungsvolle Handeln von Sicherheitsforschern und Entdeckern von Sicherheitslücken schützt. Diese Regelung muss für interne und externe Personen gelten, also auch solche, die als Mitarbeiter/innen in einem Unternehmen Sicherheitslücken in von diesem vertriebenen Waren oder Anwendungen bzw. Dienstleistungen weiter melden.

In diesem Zusammenhang sind die Auswirkungen der Neufassung des § 202a StGB (41. StrÄndG vom 07.08.2007) auf die Überprüfungsmöglichkeiten von Sicherheitslücken in Computersystemen zu prüfen, da sich mit dieser Änderung auch diejenigen strafbar machen, die mit dem Ziel, Sicherheitslücken aufzuzeigen, unbefugt in fremde Systeme eindringen, um Software-/Sicherheitslücken aufzudecken. Um sich selbst schützen zu können, müssen Bürgerinnen und Bürger und Unternehmen auf vertrauenswürdige und sichere Soft- und Hardware sowie zuverlässige Verschlüsselungssysteme zurückgreifen können.

- Wir wollen deshalb Zulassungs- und Zertifizierungsregime für vertrauenswürdige und sichere Software und Hardware fördern und ähnlich wie bei den kritischen Infrastrukturen Mindestschutzstandards für sicherheitsrelevante Soft- und Hardware setzen.
- Und wir wollen eine vertrauenswürdige und sichere Ende-zu-Ende-Verschlüsselung im Behördenverkehr und bei Sozial- und Gesundheitsdaten als Angebot verbindlich vorschreiben.
- Zukunftsprojekte, wie das Projekt „Sichere Identitäten“ im Rahmen der Hightech Strategie der Bundesregierung, müssen weiter gestärkt werden. Nur mit sicheren Identitäten können Nutzer, Bürger, Unternehmen und Behörden ihre Rechte auf informationelle Selbstbestimmung wahrnehmen. Sichere Identitäten sind Grundlage für netzbasierte Geschäftsmodelle und die Industrie 4.0 sowie ein wichtiger Faktor im Kampf gegen Auswüchse der Cyberkriminalität wie Identitätsdiebstahl oder dem Vortäuschen von Internetseiten. Ziel muss es sein, grenzüberschreitende Anwendungen bei der elektronischen Identifizierung, der qualifizierten elektronischen Signatur, des elektronischen Siegels für Unternehmen und Behörden sowie anderen elektronische Vertrauensdiensten zu ermöglichen. Entsprechend muss die Förderung ausgebaut werden.
- Wir brauchen ein Förderprogramm des BMWi zur „Weiterentwicklung vertrauenswürdiger Verschlüsselungsverfahren“, um Bürgerinnen und Bürgern aber auch Unternehmen wirksame und einfach zu nutzende Selbstschutzinstrumente an die Hand zu geben. Wenn es eine Erkenntnis aus den jüngsten Abhör- und Datenskandalen gibt, so lautet diese, dass allein sichere und vertrauenswürdige Verschlüsselungstechnologien einen weitgehenden Schutz der elektronischen Kommunikation bieten können. Dieses Projekt sollte anschließen an eine Förderung der Verschlüsselungstechnologie GnuPG des BMWi in seiner Entstehungsphase (1999 bis 2001). Heute genießt diese Verschlüsselungstechnologie hohe Akzeptanz und Vertrauen, ist Teil des IT-Grundschutzes des BSI und setzt einen wichtigen Verschlüsselungsstandard in der „freien Softwarewelt“ („Made in Germany“). Ziel dieser Förderung muss insbesondere die Weiterentwicklung und Implementierung in alle gängigen Mailprogramme sowie die einfache Nutzbarkeit für Jedermann sein.

*Wir wollen bestehende Straftatbestände vor dem Hintergrund der technologischen Entwicklung überprüfen:*

Aufgrund der schnellen Weiterentwicklung und der Dynamisierung der Technik müssen die bestehenden Straftatbestände evaluiert und gegebenenfalls gesetzgeberisch angepasst werden. So bietet nach unserer Auffassung der § 100 a Abs. 2 StPO keine hinreichende Rechtsgrundlage für die Quellen-TKÜ, weil er eine Beeinträchtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht ausreichend berücksichtigt. Zudem enthält diese Vorschrift keine Schutzvorkehrungen, um rechtlich und technisch sicherzustellen, dass die Überwachung nur die laufende Telekommunikation erfassen würde. Dazu müssten Bestimmungen in § 100 a StPO Eingang finden, die der erhöhten Eingriffsintensität und den technischen Besonderheiten der Quellen-TKÜ gerecht werden. Darüber hinaus muss eine Überprüfung des Quellcodes vor, während und nach entsprechenden Einsätzen durch die berechtigten Stellen ermöglicht werden.

Angesichts der Enthüllungen über die Ausspähaktivitäten ausländischer Nachrichtendienste sind verbindliche Abkommen notwendig, die eine Ausspähung unter EU-Mitgliedsstaaten und zwischen Partnerländern wirksam unterbinden. Insbesondere wollen wir:

- dass in Zusammenarbeit mit Unternehmen, der Wissenschaft, dem BSI und der Bundesnetzagentur (BNetzA) umfassende IT-Sicherheitskonzepte, -architekturen und -standards für Industrie 4.0 und Smart Services zum Schutz vor Wirtschaftsspionage und -sabotage entwickelt und etabliert werden. Hierbei gilt es, das Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit sowie das EU-Rahmenprogramm „Horizont 2020“ voll auszuschöpfen sowie neue innovative Forschungsansätze zu fördern;
- auf der Basis der Einigung zwischen der Europäischen Kommission und den USA über ein „EU-US Privacy Shield“ für transatlantische Datenübermittlungen darauf hinwirken, dass die Angemessenheitsentscheidung der Europäischen Kommission den Schutz von Privatsphäre und Unternehmensgeheimnissen und die staatliche Sicherheit gleichermaßen garantiert.

Berlin, den 21. Juni 2016